Cryptographically Signed License Issuance with Payment in Cryptocurrency

Perry Kundert

2022-01-25 12:32:00

Licensing software and getting paid for it has become extremely difficult, due to government, regulatory and banking interference.

The `crypto-licensing` Python module allows you automatically and securely issue licenses, and get paid in various cryptocurrencies.

Contents

1 Software Licensing Using Ed25519 Signatures

1.1 Issuing A License

To begin authoring Licenses, you need to be able to sign them. Create and save an encrypted Ed25519 keypair.

1.1.1 `authoring`: Creating an Authoring Keypair

The raw `ed25519.Keypair` from `authoring` isn't serializable, so get a `crypto_licensing` `KeypairEncrypted` and save its `str( <KeypairEncrypted> )` output to a file.

```
import crypto_licensing as cl
username = 'admin@awesome-inc.com'
password = 'password'
auth_keypair = None or cl.authoring( seed=b'\xff' * 32 ) # don't do, unless you have a random seed!
encr_keypair = cl.KeypairEncrypted( auth_keypair, username=username, password=password )
decr_keypair = cl.KeypairPlaintext( encr_keypair.into_keypair( username=username, password=password ))
[
    [ "Plaintext:", "" ],
    [ "verifying", decr_keypair['vk'] ],
    [ "signing", decr_keypair['sk'] ],
    [ "Encrypted:" ],
    [ "salt", encr_keypair['salt'] ],
    [ "ciphertext", encr_keypair['ciphertext'] ],
]
```

0	1
Plaintext:	
verifying	dqFZIESm5PURJlvKc6YE2QsFKdHfYCvjChmpJXZg0fU=
signing	//92oVkgRKbk9REmW8pzpgTZCwUp0d9gK+MKGakldmDR9Q==
Encrypted:	
salt	b26ccc242f51655b954803ce
ciphertext	c7c5dc6a8265ec8d5b242aff2b8ee9656aeb9ee8038e23615186c325ac75e193d6adfabea5dd529fd130eba9f8c40287

1.1.2 `register`: Create and save an Authoring Keypair

1.1.3 `issue`: Signing a License

A License can be as simple, free-standing authorization with no other License dependencies, or it may have a tree of sub-Licenses that must also be confirmed as valid.

1.1.4 `verify`: Confirm License (and sub-License) Validity

1.2 Using Licenses

1.2.1 `load_keys`: Find all Ed25519 Signing Keys

1.2.2 `load`: Find all Licenses

1.2.3 `check`: Find all Keys and Valid Licenses

Loads every available Ed25519 Keypairs (with the provided credentials), and all available Licenses, yielding all <Keypair>,<LicenseSigned> that are valid in the current environment.

If no valid License is available for some key found, then <Keypair>,None is yielded, allowing the caller to use the Key to issue a License if desired.

If nothing at all is yielded, then this indicates that **no** Keypairs were found; either you need to "register" (create and save) one, or provide different credentials.

1.3 Running A `crypto_licensing.licensing` Server

Supply the `username` and `password` to the `KeypairEncrypted` via environment variables `CRYPTO_LIC_USERNAME` and `CRYPTO_LIC_PASSWORD`.

2 Payment with Cryptocurrencies

3 Issuance via Web API